

## **ATTACHMENT A**

### **AFFIDAVIT**

I, Zach Bulliner, declare under penalty of perjury that the following is true and correct:

#### **Introduction**

1. I am a Special Agent with the United States Secret Service ("USSS") assigned to the Nashville Field Office, and have been employed as a Secret Service Agent for approximately four years. As part of my official duties, it is my responsibility to investigate credit card fraud, as well as other fraud cases involving access devices. Title 18, United States Code, Section 1029(a)(2) provides that it is unlawful to knowingly and with the intent to defraud traffic in or use one or more unauthorized access devices and by such conduct to obtain anything of value aggregating \$1,000 or more during any one-year period. Title 18, United States Code, Section 2(b) provides that whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal.
2. This affidavit is submitted in support of a Criminal Complaint against David Haltinner, also known as, "RevenantShadow"
3. The information contained in this affidavit is based upon my personal participation in the investigation of an individual known to me by his online identity "RevenantShadow." As explained below, I have probable cause to believe that the person known to me as "RevenantShadow" is David Haltinner. My investigation has included the Internet

correspondence in which I have engaged with “RevenantShadow,” interviews I have conducted, my examination of reports and records, and my conversations with other law enforcement officials. Because this affidavit is being submitted for the limited purpose of establishing probable cause for the issuance of an arrest warrant, it does not include all the facts I have learned during the course of my investigation.

**Investigation of “RevenantShadow”**

4. The following terms are used in this affidavit to describe the activities of “RevenantShadow” and the agents conducting the investigation of this case.
  - a. “BIN” is an acronym for “Bank Identification Number” and refers to the first six numbers of a 16- digit credit card number. Those first six numbers identify the bank that issued that credit card number. Individuals purchasing stolen credit card numbers may prefer cards issued by particular banks and may request cards with the BINs for those banks.
  - b. “CARDING” is a term which refers to the act of using stolen or compromised credit card information to obtain merchandise or any product that can be purchased with a credit card.
  - c. “CVV2” is an abbreviation for “Card Verification Value.” The CVV2 is a three- or four-digit code that typically is printed on the back of a credit card and which

provides a cryptographic check of the information embossed on the card. "CVV2" also is a term used for stolen credit card information that comes in a limited format. A CVV2 usually contains the credit card number and expiration date, the card holder's name, address, email, and phone number. CVV2s typically sell for about \$2.00 to \$3.00 a piece.

- d. "Drops" are addresses to which fraudulently ordered merchandise may be sent in order to conceal the identity of the person ordering the merchandise. A drop may be a vacant house or apartment. A drop also may be the address of a witting or unwitting accomplice who has been instructed to receive a package at one address and re-ship it to another address.
- e. "E-gold" is an Internet based payment system that allows subscribers to transfer money to other subscribers over the Internet.
- f. "IP address" is an abbreviation for Internet Protocol address. An Internet Protocol address is a unique number assigned to each computer that accesses the Internet. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 1.160.10.240 could be an IP address. An IP address may be either "static" or "dynamically assigned." A static IP address is permanently assigned to a particular user and does not change with each Internet session. A dynamically assigned IP address is one of several IP addresses

assigned to an Internet Service Provider and that, in turn, is temporarily assigned to a customer of that Internet Service Provider only for the duration of each Internet session.

- g. “TOR proxy” is an Internet-based server that enables its users to communicate anonymously via the Internet. TOR is an abbreviation for “The Onion Router,” a name given to a technique for anonymous communication over a computer network. TOR proxies may be established on Internet servers that have been compromised by hackers. TOR proxies also may be Internet servers located in foreign countries that are not easily subject to legal process from the United States. The use of TOR proxies conceals the true identity of a user behind an essentially untraceable IP address.

- 5 On January 13, 2004, Agents of the USSS in Nashville, Tennessee and the United States Postal Inspection Service (“USPIS”) in Nashville, Tennessee began a joint investigation entitled Operation Trojan Horse. Operation Trojan Horse has targeted numerous Internet websites that have been used to commit a wide range of fraudulent activities including credit card fraud, identity theft, and computer fraud. Agents of the USSS and USPIS created several usernames on these websites in order to operate on the sites in an undercover capacity and to examine suspected fraudulent activities conducted on the sites.

- 6 This case originated on April 13, 2007, while I was operating undercover on cardersmarket.com. Cardersmarket.com is an Internet-based website that is frequented by individuals engaged in credit card fraud. On April 13, 2007, I noticed a post made by “RevenantShadow” in which he advertised credit card information for sale. In the post, he stated that he was selling credit card numbers including the CVV2 for \$3 a piece. He also stated that he was selling credit card numbers without the CVV2 (hereafter referred to as “plain cards”) for \$0.10 a piece. He instructed anyone interested to email him at [revenantshadow@gmail.com](mailto:revenantshadow@gmail.com).
- 7 Continuing on April 13, 2007, I sent a ruse email to [revenantshadow@gmail.com](mailto:revenantshadow@gmail.com) for the purpose of obtaining an IP address for “RevenantShadow.” A read-receipt was attached to that email which generated a report detailing IP address information when the email was first opened and again each time it is opened subsequently.
- 8 On April 14, 2007, “RevenantShadow” opened that ruse email through a Taipei, China based IP address, 140.112.23.172, which appears to be a TOR proxy.
- 9 On April 15, 2007, “RevenantShadow” re-opened the ruse email through a Kawasaki, Japan based IP address 222.144.104.5, which also appears to be a TOR proxy.

10. On April 16, 2007, while utilizing undercover username # 1, I emailed "RevenantShadow" at revenantshadow@gmail.com and advised him that I was interested in purchasing one hundred (100) CVV2s.
11. On April 17, 2007, while utilizing undercover username # 1, I received an email from "RevenantShadow" who stated that his credit card numbers had never been used before and that he did not sell the numbers to more than one person. He further stated that I could choose any criteria for the cards. He also provided to me an E-gold account # 4082977 to use to pay him for the credit card numbers that I wanted to purchase.
12. On April 18, 2007, while utilizing undercover username # 1, I received an email from "RevenantShadow" who advised me that he could provide Visa, American Express, MasterCard, or Discover credit card numbers. In addition, he stated that he could provide numbers based on cities, states, or various other criteria.
13. On April 20, 2007, I transferred \$304.28 from an undercover E-gold account to E-gold account # 4082977, previously provided to me by "RevenantShadow."
14. Continuing on April 20, 2007, while utilizing undercover username # 1, I emailed "RevenantShadow" at revenantshadow@gmail.com and advised him that I had sent \$304.28 to his E-gold account and that I would like to order one hundred and one (101) Discover cards.

15. Continuing on April 20, 2007, while utilizing undercover username # 1, I received an email from "RevenantShadow" with 101 American Express CVV2s attached in a zip file.
16. On April 24, 2007, I transferred \$398.63 from an undercover E-gold account to E-gold account # 4082977, previously provided by "RevenantShadow."
17. Continuing on April 24, 2007, while utilizing undercover username # 1, I emailed "RevenantShadow" at [revenantshadow@gmail.com](mailto:revenantshadow@gmail.com) and advised that I had sent \$398.63 to his E-gold account and that I would like to order one hundred and thirty-three (133) Discover cards.
18. Continuing on April 24, 2007, while utilizing undercover username # 1, I received an email from "RevenantShadow" stating that he only had twenty (20) Discover CVV2s at that time.
19. Continuing on April 24, 2007, while utilizing undercover username # 1, I emailed "RevenantShadow" at [revenantshadow@gmail.com](mailto:revenantshadow@gmail.com) and advised him to send the twenty (20) Discover CVV2s and to fill the rest of the order with American Express CVV2s. I also asked him whether he would be getting more Discover numbers in the future.
20. Continuing on April 24, 2007, while utilizing undercover username # 1, I received an email from "RevenantShadow" stating that he would send the Discover and American Express

CVV2s. He also stated that because he did not have all the Discover CCV2s that I had asked for, he would also send a couple hundred plain Discover card numbers. He further advised that he had “hundreds of thousands” of plain Discover card numbers

21. Continuing on April 24, 2007, while utilizing undercover username # 1, I received an email from “RevenantShadow” with 103 American Express and Discover CVV2s, and 250 plain Discover card numbers attached in a zip file
22. Continuing on April 24, 2007, while utilizing undercover username # 1, I emailed “RevenantShadow” at revenantshadow@gmail.com and asked if there were particular BIN numbers for which he had a lot of credit card numbers.
23. On April 25, 2007, while utilizing undercover username # 1, I received an email from “RevenantShadow” in which he provided a list of all BINs he had available in his inventory of CVV2s.
24. Continuing on April 25, 2007, I forwarded the eighty-two (82) American Express account numbers that I had received for “RevenantShadow” to American Express Global Security.
25. Continuing on April 25, 2007, I was contacted by American Express Global Security and advised that all the compromised American Express account numbers that I had received from “RevenantShadow” recently were used at the business known as Listerine Dental



Direct, 201 Tabor Road in Morris Plains, New Jersey. American Express Global Security advised me that several of the credit card numbers appeared to be associated with Dentists or Dental Practices. According to a Pfizer Pharmaceutical Company website, Pfizer owns the Listerine brand

26. Continuing on April 25, 2007, while utilizing undercover username # 1, I emailed "RevenantShadow" at revenantshadow@gmail.com and asked if he would be getting access to new databases in the future.
27. Continuing on April 25, 2007, while utilizing undercover username # 1, I received an email from "RevenantShadow" in which he stated that he "was into just two different companies data" and that he planned to compromise more when he had time. "RevenantShadow" also asked me if I knew anyone trustworthy who could get him a computer with E-gold or if I knew of any merchants who would accept E-gold in payment.
28. Continuing on April 25, 2007, while utilizing undercover username # 1, I asked "RevenantShadow" if he was trying to buy a computer legitimately using E-gold, rather than carding it. I also asked what kind of computer he was seeking.
29. Continuing on April 25, 2007, while utilizing undercover username # 1, I received an email from "RevenantShadow" in which he stated that he wanted to buy a computer with E-gold, but still arrange to have it drop shipped to him.

30. Continuing on April 25, 2007, while operating undercover on cardersmarket.com, I noticed another post made by "RevenantShadow" in which he stated that he was selling a database that contained over 600,000 plain credit card numbers. He advised that he was constantly getting new numbers in and his database was getting too difficult to manage. He stated that he would sell the database for \$2000 E-gold or for the highest bid.
31. On April 26, 2007, while utilizing undercover username # 1, I emailed "RevenantShadow" at [revenantshadow@gmail.com](mailto:revenantshadow@gmail.com) and advised that I did not have enough money to buy the database but was interested in working a deal for as much of it as possible.
32. On April 27, 2007, while utilizing undercover username # 1, I received an email from "RevenantShadow" in which he indicated he was open to working something out. He further advised that he obtained around 60,000 more plain credit cards every month.
33. Continuing on April 27, 2007, while utilizing undercover username # 1, I emailed "RevenantShadow" at [revenantshadow@gmail.com](mailto:revenantshadow@gmail.com) and proposed to give him \$300, plus the computer he was seeking, in return for the database he had advertised on CardersMarket.
34. Continuing on April 27, 2007, while utilizing undercover username # 1, I received an email from "RevenantShadow" in which he declined my offer stating that he had carded a laptop

the previous night and it seemed to have gone through. He advised me that if it was unsuccessful he would let me know.

35. Continuing on April 27, 2007, while utilizing a new undercover username (undercover username # 2), I emailed "RevenantShadow" at [revenantshadow@gmail.com](mailto:revenantshadow@gmail.com) and advised that I was interested in purchasing the database he had advertised on CardersMarket. I also inquired if there was a way to obtain the matching CVV2s for the numbers.
36. Continuing on April 28, 2007, while utilizing undercover username # 2, I received an email from "RevenantShadow" stating that the database was still available and that he was unable to obtain the CVV2s for the numbers because "the place that I get them from doesn't use the CVV."
37. On April 28, 2007, while utilizing undercover username # 1, I received an email from "RevenantShadow" stating that his attempt to card a laptop had failed. He further advised that if I could get him a MacBook Pro laptop computer, he would accept it in trade for the database he had advertised on CardersMarket.
38. Continuing on April 28, 2007, while utilizing undercover username # 2, I emailed "RevenantShadow" at [revenantshadow@gmail.com](mailto:revenantshadow@gmail.com) and offered \$1200 for the database he had advertised on CardersMarket.

39. Continuing on April 28, 2007, while utilizing undercover username # 2, I received an email from "RevenantShadow" accepting my offer of \$1200 and stating that he could upload the data file containing the credit card numbers to an FTP server from which I could then download it.
40. Continuing on April 29, 2007, while utilizing undercover username # 2, I emailed "RevenantShadow" at [revenantshadow@gmail.com](mailto:revenantshadow@gmail.com) and advised him that I would open a new E-gold account in order to send him the \$1200. I further stated that he could send the data file containing the credit card numbers to me via an FTP link as he had proposed.
41. On April 30, 2007, while utilizing undercover username # 1, I emailed "RevenantShadow" at [revenantshadow@gmail.com](mailto:revenantshadow@gmail.com) and advised that I accepted his offer and would get to work on obtaining a MacBook Pro laptop computer.
42. Continuing on April 30, 2007, while utilizing undercover username # 2, I received an email from "RevenantShadow" in which he provided the E-gold account # 4082977 to which my payment could be sent.
43. Continuing on April 30, 2007, while utilizing undercover username # 2, I received an email from "RevenantShadow" suggesting that we use the website [www.sendthisfile.com](http://www.sendthisfile.com) (a website that provides FTP servers to and from which data may be uploaded and downloaded) because it is free and it supports proxies such as Tor, Squid, and Privoxy.

44. On May 1, 2007, while utilizing undercover username # 2, I emailed "RevenantShadow" at revenantshadow@gmail.com and stated that I wanted to make sure that the numbers in the database he was going to sell were good numbers and not dead. I also asked if he knew what kind of credit limits the cards had.
45. Continuing on May 1, 2007, while utilizing undercover username # 2, I received an email from "RevenantShadow" in response to my inquiry. He stated that the credit card numbers are known to be valid in the last 60 days. He said he captured them on the wire during the authorization process and that he did not capture declined cards. He said all the ones that he already had sold had been removed from the batch he was selling to me, so all the cards he would be sending me would be virgin cards. He said the credit limits seemed rather broad. He said that he had used a few of the credit card numbers to buy some stuff, and that one had a \$200 limit, one had a \$1500 limit, and that he did not reach the limit on the other card he had used. He also offered to send me a BIN list for the cards he would be sending to me.
46. On May 2, 2007, while utilizing undercover username # 2, I received an email from "RevenantShadow" stating that he was writing a script that would go through the database and count the BINs. He stated he would send the BIN list once he was done.
47. Continuing on May 2, 2007, I obtained records from Google, Inc relating to the email address revenantshadow@gmail.com. Those records revealed the IP address used to set up the

account [revenantshadow@gmail.com](mailto:revenantshadow@gmail.com)., which was 128.197.11.30. Those records also revealed IP addresses used subsequently by "RevenantShadow" to access that email account.

48. Continuing on May 2, 2007, I conducted a WHOIS search on IP address 128.197.11.30, which indicated this IP address resolves to Boston University. I contacted the Boston University Intrusion Response Team and was advised that this IP address was a known TOR proxy. The IP addresses used subsequently by "RevenantShadow" to access that email account also appear to be other TOR proxies.
49. Continuing on May 7, 2007, I transferred \$1,200 from an undercover E-gold account to E-gold account # 4082977, previously provided to me by "RevenantShadow." While utilizing undercover username #2, I sent an email to "RevenantShadow" advising him that I had transferred the \$1,200 to his E-gold account.
50. On May 7, 2007, while utilizing undercover username # 2, I received an email from "RevenantShadow" stating that he had posted the file containing the credit card numbers on the website [www.sendthisfile.com](http://www.sendthisfile.com).
51. On May 7, 2007, I accessed the website [www.sendthisfile.com](http://www.sendthisfile.com) from Nashville, Tennessee and downloaded the file containing the credit card numbers that "RevenantShadow" had posted for me. The file was very large, approximately 24.7 megabytes. Based upon the portion of the file that I attempted to print, I estimate the file to be approximately 5,000 pages

of information. Based upon an automated count of the number of credit card numbers in the file, it appears that the file contains approximately 637,000 credit card numbers. The information in the file includes names, addresses and corresponding credit card numbers.

52 I identified twenty credit card numbers from that data file that appeared to be issued by American Express. I provided those credit card numbers and the names and addresses associated with each of them to American Express Global Security. American Express Global Security advised me that fourteen of those credit card numbers recently were used at an online Disney movie business.

53 On May 8, 2007, while utilizing undercover username # 1, I sent an email to "RevenantShadow" and advised him that I expected to have the MacBook Pro laptop computer by the following day and asking where he wanted me to send it.

54 On May 9, 2007, while utilizing undercover username # 1, I received an email from "RevenantShadow" advising me to send the MacBook Pro computer to his "drop ship" at "Gary Cornerman, 120 North Commercial Street, Neenah, Wisconsin 54956."

55 I researched the address, "120 N. Commercial Street, Neenah, WI," and found that the business at this address is known as Alta Resources. Based upon my review of an Alta Resources website and other Internet resources, I believe that Alta Resources provides call

center and fulfillment services to several nationally recognized businesses. Included among a list of twenty-one of its clients on the Alta Resources web page are the Disney Movie Club and Pfizer, which owns the Listerine brand. According to an October 15, 2004 article in the Business Journal of Milwaukee, Alta Resources employed approximately 1000 people at that time. I believe some employees of Alta Resources would have access to a large number of credit card numbers for customers of both the Disney Movie Club and Listerine Dental Direct and that Alta Resources may be the point of compromise for the credit card numbers that I purchased from "RevenantShadow."

56. On May 10, 2007, I purchased a MacBook Pro computer, serial number W8718028W0H, from CompUSA for \$ 2,731.24.
57. On May 10, 2007, United States Magistrate Judge John S. Bryant of the Middle District of Tennessee issued a warrant authorizing the USSS to install on a Remote Collection Agent (RCA) onto the MacBook Pro computer before we sent it to "RevenantShadow." The RCA that we were authorized to install is a software tool provided to us by a private company known as Absolute Software Corporation. Absolute Software Corporation is engaged in the business of providing recovery services for stolen laptop computers to individuals and organizations. The RCA tool provided to us by Absolute Software Corporation was designed to covertly contact the Absolute Software Corporation monitoring center and report the IP address of any Internet connection made using the any computer on which it is installed. The RCA provided by Absolute Software Corporation allows Absolute Software Corporation to



track the location of any computer on which it is installed. The RCA forces the computer to contact the Absolute Software Corporation's monitoring center by two different methods. When the computer is connected to a phone line, the RCA causes the computer to call the Absolute Software Corporation monitoring center. The monitoring center logs and archives the electronic serial number of the computer, the date and time of the call and originating telephone number of the call. With this information, Absolute Software Company may pinpoint the precise physical location of the computer, even if the telephone line is equipped with caller identification blocking. When the computer is connected to the Internet, the RCA forces the computer to send a message to the monitoring center. This message, like all Internet messages, contains the IP address of the sending computer. The RCA causes the computer to contact the Absolute Software Corporation's monitoring center at pre-determined intervals, without interfering with the normal use of the computer and without alerting the user of the computer that it is contacting the monitoring center.

58. I also am advised by Absolute Software Corporation, that the RCA collects information about the physical architecture of the computer and the software install base to properly identify the computer. As noted, the RCA collects the means of the computers connection to the Internet, such as IP addresses. If there is a user defined email address (as distinguished from a web-based email address) the RCA can capture that information. However, the RCA does not collect the content of electronic communications or data that the user of the computer creates, stores or sends through email, chat sessions or instant messaging.

59. On May 10, 2007, Special Agent Nate Landkammer of the USSS in the Middle District of Tennessee installed the RCA provided to by the Absolute Software Corporation onto the MacBook Pro computer, serial number W8718028W0H.
60. On May 11, 2007, while utilizing undercover username #1, I received an email message from "RevenantShadow" asking that I send the computer overnight (for delivery on Monday May 14, 2007) or to wait to send it until later in the week because RevenantShadow's "shipper" said he was going to be gone for a couple of days.
61. On May 11, 2007, that computer then was sent via Federal Express by Special Agent Landkammer addressed to Gary Cornerman at 120 N. Commercial Street in Neenah, Wisconsin for delivery on May 14, 2007. The box in which the computer was sent was a brown cardboard box with "Fed Ex" printed in purple letters on the side of the box. The dimensions of the box were 17 inches x 17 inches x 7 inches. The shipping label was in a clear plastic pouch on top of the box. The box was sealed with clear packaging tape.
62. On May 11, 2007, while utilizing undercover username # 1, I sent an email to "RevenantShadow" and advised him that the computer had been sent to the address that he had instructed. I provided "RevenantShadow" with the Federal Express tracking number so that he could follow the progress of its delivery to the address he had provided to me

63. On May 12, 2007, "RevenantShadow" sent an email to undercover username # 1 stating that based upon the Federal Express tracking number that had been provided to him that he had posted the file containing the credit card numbers on the website [www.sendthisfile.com](http://www.sendthisfile.com).
64. On May 13, 2007, I accessed the website [www.sendthisfile.com](http://www.sendthisfile.com) from Nashville, Tennessee and downloaded the file containing the credit card numbers that "RevenantShadow" had posted for him. The file was the same size as the large file sent to undercover username # 2, approximately 24.7 megabytes, on May 7, 2007 and appears to contain identical information.
65. On May 14, 2007, at approximately 8:30 a.m., Special Agent Doug Farrell of the Milwaukee Field Office of the USSS established surveillance at Alta Resources, 120 N. Commercial, Rear Door (Delivery Entrance) Neenah, Wisconsin.
66. On May 14, 2007 at approximately 9:15 a.m., Agent Farrell observed a FedEx truck unload it's items for delivery at 120 N. Commercial. Agent Farrell observed the following items were carried into Alta Resources by the driver:
- a. One (1) FedEx mail crate containing several FedEx envelopes
  - b. One (1) "LARGE" FedEx box (white in color)
  - c. One (1) FedEx box (brown in color)

67. On May 14, 2007, at approximately 9:30 a.m., Special Agent Scott Bates of the Milwaukee Field Office conducted a FedEx Tracking Number inquiry via the internet which indicated the subject package, tracking #8595 1998 2890 was delivered at 9:18 a.m.
68. On May 14, 2007 at approximately 12:45 p.m., Agent Farrell and Special Agent Jeremy Eichberger of the Milwaukee Field Office were conducting a surveillance in the Alta Resources parking garage when they observed a white male (later identified as David U. Haltinner, DOB: 12/17/1981) carrying a FedEx box (brown in color). Specifically, Mr. Haltinner entered the parking garage from the pedestrian way entrance which connects directly to Alta Resources. Mr. Haltinner walked to a blue Jeep, Wisconsin registration "363JTB", and placed the package in the rear cargo area. Mr. Haltinner then exited the parking garage and had a cigarette in the designated smoking area before he returned to Alta Resources. According to Agent Farrell, the aforementioned FedEx box was similar in size and color to the package he saw being delivered at 9:15 a.m.
69. On May 14, 2007, at approximately 1:00 p.m., Agent Eichberger looked into the blue Jeep's rear cargo area and observed a FedEx box (brown in color) placed face down so that no shipping label was visible. Agent Eichberger observed that the FedEx box appeared to be sealed in its original state with clear packaging tape.
70. On May 14, 2007, at approximately 1:00 p.m., Special Agent Jim Schultz of the Milwaukee Field Office conducted a Wisconsin Department of Transportation (WDOT) registration

inquiry for the blue Jeep. WDOT records indicated the Jeep was registered to: David U Haltinner (DOB: 12/17/1981); 1297 Lakeview Lane; Menasha, WI 54952; 1994 Jeep, blue in color.

71. On May 14, 2007, at approximately 3:59 p.m., while utilizing undercover username #1, I received an email from "RevenantShadow" advising me that his "shipper" had received the package and that he ("RevenantShadow") should have it in a day or two.
72. On May 14, 2007, at approximately 5:05 p.m., Mr. Haltinner departed the Alta Resources parking garage in his blue Jeep.
73. On May 14, 2007, at approximately 5:15 p.m., Special Agent Timothy Flannery of the Milwaukee Field Office observed Mr. Haltinner arrive at 1297 Lakeview Lane, Menasha, Wisconsin. Mr. Haltinner drove directly from Alta Resources to Lakeview Lane. Upon arrival at 1297 Lakeview Lane, Agent Flannery observed Mr. Haltinner remove the FedEx box from the rear cargo area of his Jeep and place it on the floor inside his garage. Mr. Haltinner then entered the residence at 1297 Lakeview Lane, but left the garage door open with the FedEx box in view from the street. Agent Flannery also observed two other vehicles parked in the garage at 1297 Lakeview Lane.
74. On May 14, 2007, at approximately 5:45 p.m., Agent Eichberger observed the FedEx box in the garage at 1297 Lakeview Lane and noted that it appeared to have been opened. Agent

Eichberger also observed that the two vehicles in the garage had Wisconsin registrations "118DXE" and "DUHJEEP". A WDOT inquiry of the registrations indicated the following:

Wisconsin Registration "118DXE"  
Angelina M. Bloomer  
1297 Lakeview Lane  
Menasha, WI 54952  
2006 Jeep Grand Cherokee, blue in color

Wisconsin Registration "DUHJEEP"  
David U. Haltinner  
1297 Lakeview Lane  
Menasha, WI 54952  
1999 Jeep

75. On May 14, 2007, Agent Schultz obtained an electronic image of Mr. Haltinner's Wisconsin Driver's License photograph. Agent Farrell, Agent Flannery, and Agent Eichberger identified Mr. Haltinner's Driver's License image as the same person handling the aforementioned FedEx box throughout the day on May 14, 2007.
76. On May 14, 2007, Agent Farrell conducted a Winnebago County Tax Record search for 1297 Lakeview Lane, Menasha, Wisconsin. Winnebago Tax records indicated that Mr. Haltinner was the current owner at 1297 Lakeview Lane, Menasha, Wisconsin.
77. On May 15, 2007, Agent Landkammer and I made a digital photograph of the type of Federal Express box that Agent Landkammer had used to ship the computer to "Gary Cornerman" and I emailed that photograph to Agent Eichberger. Agent Eichberger and Agent Ferrell

confirmed to me that this was the same type of box that they saw in the possession of Mr. Haltinner.

78. On May 16, 2007, I obtained records from SendThisFile.com which show that both of the large files containing credit card numbers uploaded to SendThisFile.com by "RevenantShadow" on May 7, 2007 and on May 12, 2007 came from the IP address 208.49.58.254. I conducted a WHOIS search on IP address 208.49.58.254, which indicated this IP address resolves to "ns4.altaresources.com." This appears to be a server associated with Alta Resources.
79. On May 17, 2007, while utilizing undercover username # 1, I received an email from "RevenantShadow" in which he advised me that he had just received the computer that we had sent to him and that he had not yet had an opportunity to use it.
80. On May 18, 2006, I obtained records from Amazon.com showing four suspicious orders for merchandise to be shipped to the address of Alta Resources at 120 N. Commercial Street in Neenah Wisconsin. The first three of these suspicious orders were shipped to "Gary Cornerman," the same name to which "RevenantShadow" instructed me to send the MacBook Pro computer. The first of these three shipments contained "Star Trek Voyager - The Complete Seasons 1-7" purchased for \$696.99 from Amazon.com on May 3, 2007 and shipped on May 3, 2007. The second of these three shipments contained a "VGA to Component Video Scan Converter 640X480 1600X1200 for HDTV" purchased for \$194.86

from Amazon.com on May 7, 2007 and shipped on May 7, 2007. The third of these three shipments contained a "Toshiba 32HLV66 32" Diagonal TheaterWide 16:9 Integrated HD LCDVD IV" purchased for \$878.88 from Amazon.com on May 7, 2007 and shipped on May 8, 2007. These last two orders were placed on the same day that I transferred \$1,200 to the E-gold account of "RevenantShadow." Two of these orders included in the "Gift Message Field" the words "Thank you for shopping at Gold Stores!" Gold Stores is an Internet-based retailer that accepts payment in E-gold. The Gold Stores web site home page states, "Welcome to GoldStores.com Now you can shop and pay for your purchases with either E-gold, E-bullion, Pecunix ... Here you will find the same great variety of products plus the added convenience of e-currency." The Gold Stores web site roughly approximates the Amazon.com web site, except with a general mark-up of approximately 10% over Amazon.com prices. All three of these shipments to "Gary Cornerman" were paid for with the same Visa credit card number issued to Arthur Budovsky of Manchester, New Hampshire.

81. I obtained records from E-gold for the E-gold account number provided to me by "RevenantShadow" for the period from February 10, 2007 through April 29, 2007. The "POC", which I interpret to mean "Point of Contact," for that account is listed as "Gary Cornerman." The address listed on those records for "Gary Conerman" is an invalid address in Beverly Hills, California. Those records show that \$829.94 was paid from that E-gold account to Gold Stores on April 27, 2007. I believe that this payment to Gold Stores was to cover the cost of the "Star Trek Voyager - The Complete Seasons 1-7" purchased for \$696.99.



from Amazon.com on May 3, 2007, plus a mark-up charged by Gold Stores. I have not yet obtained the records for this E-gold account for the period between April 29, 2007 through May 7, 2007 and I have not yet been able to determine if there were payments from the E-gold account to Gold stores that would cover the remaining two Amazon purchases shipped to "Gary Cornerman."

82. Based upon these facts, I believe that Mr. Budovsky operates the Gold Stores website, accepts orders for merchandise and payment with money from E-gold accounts, orders the merchandise from Amazon.com for shipment to his customers and pays for the merchandise with his own credit card. This process preserves the anonymity of Gold Stores' customers who want to spend the money in their E-gold accounts.
83. The fourth suspicious order placed with Amazon.com was an order for an "Apple MacBook Pro MA610LL/a Notebook PC" at a cost of \$2,499.99 placed on May 11, 2007 for shipment to another name at 120 N. Commercial Street in Neenah, Wisconsin. This order was cancelled by Amazon.com because it appeared to be fraudulent. This is the same type of computer that "RevenantShadow" requested from me. According to Amazon.com records, this order was billed to a Visa credit card for an individual that appears to be a dentist in the Milwaukee, Wisconsin area. According to Amazon.com records the email address provided by the person who placed this order was "bigstuff567@yahoo.com." According to records that I have obtained from Google, Inc., the email address, bigstuff567@yahoo.com is a secondary email address associated with the email account of revenantshadow@gmail.com.

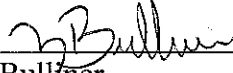
Also, the BIN (first six digits) of the Visa card number used to place this order was on a list of BINs that "RevenantShadow" sent to me on April 25, 2007. Based upon these facts, I believe that in addition to selling stolen credit card information, "RevenantShadow" has attempted to use stolen credit card information to purchase merchandise for delivery to the business address of Alta Resources and that the Visa Card number for the Milwaukee area dentist may have been obtained from a transaction by the dentist with Listerine Dental Direct

84. On May 22, 2007, a United States Magistrate Judge in Green Bay, Wisconsin issued search warrants authorizing searches of the residence of Mr. Haltinner at 1297 Lakeview Lane in Menasha, Wisconsin and the business offices of Alta Resources at 120 N. Commercial Street, in Neenah, Wisconsin.


85. On May 24, 2007, Agents of the Milwaukee Field Office executed the search warrant at the residence of Mr. Haltinner. Among the items of evidence seized pursuant to that search warrant was:

- a. A MacBook Pro computer box bearing the serial number W8718028W0H;
- b. A brown cardboard box with "Fed Ex" printed in purple letters on the side of the box, approximately 17 inches x 17 inches x 7 inches, with the shipping label removed.
- c. A set of DVDs entitled "Star Trek Voyager - The Complete Seasons 1-7;"
- d. Approximately eleven laptop computers and one desktop computer, but not the MacBook Pro computer that we sent to "Gary Cornerman."

86. Based on the facts recited above, I have probable cause to believe that David Haltinner is  
"RevenantShadow" and that David Haltinner has violated 18 U.S.C. §§ 2 and 1029(a)(2).

  
\_\_\_\_\_  
Zach Bullner  
Special Agent  
United States Secret Service

Subscribed and sworn before me this 24th day of May, 2007

  
\_\_\_\_\_  
John S. Bryant  
U.S. Magistrate Judge  
Middle District of Tennessee